

REMARKS

The Examiner is thanked for the performance of a thorough search. By this response, Claims 1, 2, 28, 34, 42, 43, 48, and 54 have been amended. No claims have been canceled or added. Hence, Claims 1–6 and 28–61 are pending in this application.

The amendments to the claims do not add any new matter to this application, and are supported by the Specification. The amendments to the claims were made to improve the readability and clarity of the claims and not necessarily for any reason related to patentability.

All issues raised in the Office Action are addressed hereinafter.

I. CLAIMS 1, 28, 33-37, 42, 48, 53-57—GREEN

Claims 1, 28, 33-37, 42, 48, 53-57 are rejected under 35 U.S.C. § 102(b) as allegedly anticipated by U.S. Patent No. 6,003,084 (hereinafter “*Green*”). Applicants traverse the rejection. Reconsideration is respectfully requested.

CLAIM 1

Claim 1, as set forth in the listing of claims, recites “performing, at [a] network entity, the computer-implemented steps of:”

monitoring the network entity;
periodically **evaluating, at the network entity, one or more
specified conditions of the same network entity**;
when one or more of the specified conditions are satisfied, then:
gathering specified information from the network entity;
**preparing a message that includes the specified
information and the specified conditions that
were satisfied**; and
**sending the message to one of a management
application or a management proxy.**

At least the above-bolded features are neither taught nor suggested by the cited reference.

Green describes a “secure network proxy for connecting clients.” *Green* at title. *Green*’s proxy “monitors connection requests” between requestors and servers. Under certain conditions, the proxy will close connections, while under other conditions the proxy will setup

and maintain a transparent connection through the proxy. *Green* at abstract. While *Green*'s proxy does appear to monitor incoming connection requests **from other network entities**, *Green*'s proxy does not appear to do any monitoring of "**conditions of the same network entity**." Nor does *Green* teach that the proxy sends messages containing information gathered from the proxy to other network entities. For at least these reasons, *Green* fails to teach or suggest a number of features of Claim 1.

- (1) *Green* does not disclose a network entity that "evaluat[es], at the network entity, one or more specified conditions of the same network entity"

Claim 1 recites a "network entity performing the step[] of . . . evaluating, at the network entity, one or more specified conditions of the same network entity." For example, a computer implementing the method of Claim 1 may implement such a step via the self-monitoring and evaluation of various events and other conditions **of itself**.

By contrast, *Green* neither teaches nor suggests such a step. The Office Action alleges that *Green* teaches a similar step in *Green* at col. 8, lines 14–24 and FIG. 3B because "in a proxy device, data is conformed with predefined conditions and is monitored by a connection manager." However, this passage of *Green* states that a connection manager at the proxy monitors "transport data" from a client. *Green* at col. 8, lines 16–17. While this "transport data" is monitored for "conformance with predefined conditions," *Green* at col. 8, lines 19–20, the transport data reflects conditions of a client network entity, not the proxy network entity that is monitoring and evaluating the data. At best, then, *Green* provides that a network entity may monitor and evaluate data sent to it from other network entities for predefined conditions. *Green* therefore does not teach a "**network entity performing the step[] of . . . evaluating, at the network entity, one or more specified conditions of the same network entity**," as recited in Claim 1.

- (2) *Green*'s alleged "message" contains neither the alleged "specified information" nor any information about "the specified conditions that were satisfied."

Claim 1 recites that, "when one or more of the specified conditions are satisfied," the network entity "prepar[es] a message that includes the specified information and the specified conditions that were satisfied." For example, a computer implementing the method of Claim 1 may implement such a step by, in response to determining that the conditions for an alarm event

have been satisfied, preparing a message indicating those satisfied conditions along with other information gathered from the computer.

The Office Action alleges that *Green* teaches such a step at *Green*, col. 10, lines 28–40, because “a message after being given an authentication information with digital signature is sent to the proxy filter.” The allegation is incorrect. The only message that appears in this passage of *Green* is an X.500 BIND request. The only information that *Green* describes this X.500 BIND request as containing is “authentication information.” **Authentication information in an X.500 BIND request is not information about “specified conditions [of the network entity] that were satisfied.” Nor is the authentication information “specified information” gathered by the alleged network entity (i.e. the proxy) in response to the satisfaction of those specified conditions.** The authentication information is not even the information that the Office Action alleges that the proxy gathers to satisfy Claim 1’s step of “gathering specified information.” See *Office Action* at 3 (apparently alleging that the proxy gathers “calling information” in *Green* at col. 10, lines 10–14 in response to determining that specified conditions are satisfied).

In fact, there is not any message in *Green* that includes both (1) information about conditions that were satisfied at a network entity and (2) information gathered from that same network entity in response to determining that those conditions were satisfied. Accordingly, *Green* neither teaches nor suggests “preparing a message that includes the specified information and the specified conditions that were satisfied.”

(3) *Green*’s alleged “message” is not sent by the alleged “network entity.”

Claim 1 recites that, “when one or more of the specified conditions are satisfied,” the network entity “send[s] the message to one of a management application or a management proxy.” For example, a computer implementing the method of Claim 1 may implement such a step by, in response to determining that the conditions for an alarm event have been satisfied, sending the example message from argument (2) above.

Again, the Office Action alleges that *Green* teaches such a step at *Green*, col. 10, lines 28–40. As discussed above, the only message that appears in this passage of *Green* is an X.500 BIND request. However, **the X.500 BIND request is sent from a client, not the proxy. Since the Office Action consistently alleges that the “proxy” is the network entity performing the steps of Claim 1, Claim 1’s step of “sending the message to one of a management**

application or a management proxy” cannot be satisfied by a client sending a message to the proxy.

A proper anticipation rejection requires a single prior art reference to disclose each and every feature of a claim, *arranged as in the claim*. *E.g.* Net Moneyin, Inc. v. Verisign, Inc., et al. No. 2007-1565 (Fed. Cir. October 20, 2008) (slip op. at 3). For at least the foregoing reasons, *Green* fails to teach or suggest at least one element of independent Claim 1. Therefore, *Green* does not anticipate Claim 1 under 35 U.S.C. § 102. Reconsideration is respectfully requested.

CLAIM 28

Claim 28, as set forth in the listing of claims, recites a method for a network element to initiate notification about an anomalous condition, comprising:

at the network element or a proxy server, performing the computer-implemented steps of:
receiving first definitions of one or more triggers, each comprising one or more conditions;
receiving second definitions of report information;
determining that at least one of the one or more triggers defined by the first definitions is satisfied, and in response thereto, initiating communication of at least some of the report information defined by the second definitions to a management proxy or a management application.

Among other purposes, the method of Claim 28 allows a network entity to receive instructions from, for instance, a management application, regarding conditions that the network entity should monitor, along with reporting data that the network entity should send to the management application when the conditions are satisfied. In an embodiment, these instructions enable the management application to configure the monitoring behavior of a network device that is employing, for instance, the monitoring technique recited in Claim 1.

By contrast, *Green* does not appear to teach or suggest any of the steps of Claim 28. About the only similarity between the method of Claim 28 and *Green's* techniques is that both potentially involve proxies.

(1) Green does not disclose “receiving first definitions of one or more triggers, each comprising one or more conditions”

Claim 28 recites “receiving first definitions of one or more triggers, each comprising one or more conditions.” For example, a computer implementing the method of Claim 28 may implement such a step by receiving a message that informs the computer of one or more triggers, each trigger comprising one or more conditions to be evaluated by the computer.

The Office Action alleges that *Green* teaches such a step in *Green* at col. 8, lines 14–24 and FIG. 3B, because “in a proxy device, data conformed with predefined conditions is monitored by a connection manager.” The Office Action is incorrect. Even if this passage of *Green* did describe “in a proxy device, data conformed with predefined conditions is monitored by a connection manager,” such a description does not teach or suggest Claim 1’s step of “receiving first definitions of one or more triggers, each comprising one or more conditions.” While the passage describes “predefined conditions,” these conditions are not part of “triggers” whose definitions are received by the proxy. In fact, there is absolutely no description in *Green* of the proxy ever receiving any data that defines triggers that comprise these conditions. Accordingly, *Green* cannot teach or suggest “receiving first definitions of one or more triggers, each comprising one or more conditions.”

(2) Green does not disclose “receiving second definitions of report information.”

Claim 28 recites “receiving second definitions of report information.” For example, a computer implementing the method of Claim 28 may implement such a step by receiving a message that defines for the computer what information should be reported in the event one of the triggers defined in the first definitions is satisfied.

The Office Action alleges that *Green* teaches such a step in col. 3, lines 29–33 and 35–43 because “the poller checks continuously network interface by sending out poller query message, when a message is polled, the proxy sends another message stating an interface is reachable.” The allegation is clearly incorrect. *Green* col. 3, lines 29–33 and 35–43 state:

The problem with this simple IP transparent bridge solution is that it can only `filter` information based on the IP addresses contained within the data. IP address spoofing is very easy, therefore this solution alone is not secure enough for the needs of securing an OSI application.

The transparent relay functionality must be moved up higher again, this time to the OSI Transport layer service. The transport layer over IP is TCP. A TCP transparent relay solution would look for data on specific TCP ports. The TCP bridge would filter based on a specific TCP port which generally maps to a unique application. The problem however, is that the OSI applications are not required to operate on any specific TCP port.

This passage clearly does not teach that the “the poller checks continuously network interface by sending out poller query message, when a message is polled, the proxy sends another message stating an interface is reachable,” as alleged by the Office Action.

Moreover, even if this passage contained such a teaching, such a teaching has absolutely no relevance to the claimed step of “receiving second definitions of report information.”

Further, this passage makes no mention of “report information,” much less of any device receiving data defining the report information. Nor does any other aspect of *Green* teach or suggest Claim 1’s step of “receiving second definitions of report information.”

- (3) *Green* does not disclose that in response to “determining that [a] trigger[] . . . is satisfied . . . initiating communication of at least some of the report information . . . to a management proxy or a management application.”

Claim 28 recites that in response to “determining that at least one of the one or more triggers defined by the first definitions [received by the network entity] is satisfied,” the network entity will communicate “at least some of the report information defined by the second definitions” received by the network entity. The Office Action alleges that *Green* discloses such a step for the same reasons as discussed above in argument (2).

As discussed above, the relied-upon passage of *Green* clearly does not teach what it is relied upon to teach. Moreover, **the relied-upon passage of *Green* does not discuss any of the following elements recited in Claim 28: triggers or the satisfaction thereof, report information, sending report information in response to satisfying triggers.**

For at least the foregoing reasons, *Green* fails to teach or suggest at least one element of independent Claim 28. Therefore, *Green* does not anticipate Claim 28 under 35 U.S.C. § 102. Reconsideration is respectfully requested.

CLAIM 34

Claim 34, as set forth in the listing of claims, recites “a method for a network element to initiate notification to a management point about an anomalous condition.” Among other purposes, the method enables a network entity to receive “management requests” that have been pooled for it at a management gateway in accordance with, for example, certain steps recited in the method of Claim 2 (see section II below). The method comprises the computer-implemented steps of:

requesting a management gateway that is communicatively coupled to the network element **to provide one or more application requests for the network element that have been stored at the management gateway** by an application;
in response to said requesting, receiving from the management gateway at least a particular application request;
in response to receiving the particular application request, initiating at the network element a communication session between the network element and the management application for enabling the network element to reply to the application request.

At least the above-bolded features are neither taught nor suggested by *Green*.

- (1) *Green* does not disclose a request “to provide one or more application requests for the network element that have been stored at the management gateway.”

Claim 34 recites a request “to provide one or more application requests for the network element that have been stored at the management gateway.” The Office Action alleges that *Green* teaches such in *Green* at col. 9, lines 17–19, because “a proxy passes through the application of OSI protocol by using application gateway solution.” The cited part of *Green* states:

Additionally, it allows support of X.500 DISP sessions through the system. This would not be possible with the full DSA application gateway solution.

This passage describes nothing more than the fact that *Green*’s solution allows the support of X.500 DISP sessions, which would not be possible in a DSA application gateway. **Clearly, the**

cited passage does not teach that “a proxy passes through the application of OSI protocol by using application gateway solution.”

More importantly, neither statement has any relevance to Claim 34. Neither statement involves any kind of request, much less a request issued by a network entity to a management gateway “to provide one or more application requests . . . that have been stored at the management gateway.”

(2) *Green* does not disclose that “in response to [the request for application requests]” the network entity “receive[s] from the management gateway at least a particular application request.”

Claim 34 recites “in response to said requesting, receiving from the management gateway at least a particular application request.” *Green* does not teach or suggest such a step because *Green* does not teach that a network entity sends a request “to provide one or more application requests for the network element that have been stored at the management gateway.”

For at least the foregoing reasons, *Green* fails to teach or suggest at least one element of independent Claim 34. Therefore, *Green* does not anticipate Claim 34 under 35 U.S.C. § 102. Reconsideration is respectfully requested.

CLAIMS 42, 48, AND 54

Each of independent Claims 42, 48, and 54 also recites features argued above with relation to Claims 1, 28, or 34, although Claims 42, 48, and 54 are expressed in another format. Because each Claims 42, 48, and 54 has at least one of the features described above for Claims 42, 48, and 54 each of Claims 42, 48, and 54 is therefore allowable over *Green* for at least one of the same reasons as given above for Claims 1, 28, or 34. Reconsideration is respectfully requested.

CLAIMS 33, 35–37, 49–53, AND 55–57

Each of Claims 33, 35–37, 49–53, and 55–57 depends from Claims 1, 28, 34, 42, 48, or 54, and includes each of the above-quoted features of its respective parent claim by dependency. Thus, *Green* also fails to teach or suggest at least one feature found in Claims 33, 35–37, 49–53, and 55–57. Therefore, *Green* does not anticipate Claims 33, 35–37, 49–53, and 55–57. Reconsideration of the rejection is respectfully requested.

In addition, each of Claims 33, 35–37, 49–53, and 55–57 recites at least one feature that independently renders it patentable. However, to expedite prosecution in light of the fundamental differences already identified, further arguments for each independently patentable feature of Claims 33, 35–37, 49–53, and 55–57 are not provided at this time. Applicants reserve the right to further point out the differences between the cited art and the novel features recited in the dependent claims.

II. CLAIMS 2–6, 29–32, 38–41, 43–47, 49–52, AND 58–61—GREEN IN VIEW OF DAVIES

Claims 2–6, 29–32, 38–41, 43–47, 49–52, and 58–61 were rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over Green (“*Green*”) U.S. Patent No. 6,003,084, in view of Davies (“*Davies*”) U.S. Patent No. 6,058,420. Applicants traverse the rejection. Reconsideration is respectfully requested.

CLAIM 2

Claim 2 recites “a method of managing a network entity that is initiated by the network entity.” Among other purposes, the method of Claim 2 is useful in facilitating the management of a network entity by a management application that is not directly connected to the network entity. Accordingly, the management application sends requests related to the network entity to a management proxy. The management proxy creates and pools management requests based on these requests. The management proxy delivers the management requests to the network entity when the network entity polls the management proxy for the requests. The method comprises “performing, at a management proxy, the computer-implemented steps of:”

- receiving a request from a management application for interaction with the network entity;
- based at least upon the request from the management application, creating a management request;
- storing said management request in the management proxy while awaiting a poll for the management request from the network entity;
- receiving a poll message from the network entity, said poll message requesting from the management proxy any

available management requests applicable to the network entity;
in response to the poll message:
selecting one or more management requests stored in the management proxy that match the network entity;
and
delivering the selected one or more management requests to the network entity;
wherein the management proxy is external to the management application and the network entity.

The combination of *Green* and *Davies* fails to teach or suggest the method of Claim 2 for at least the following reasons.

(1) *Green*'s "connection request" is received from the requestor, not "created" at the proxy

Claim 2 recites "based at least upon the request from the management application, creating a management request." The Office Action alleges that *Green* discloses a similar element in *Green* at col. 10, lines 8–12 because "a request has the source and destination addresses on it." This statement has no relevance to creating a management request.

Moreover, the Office Action apparently contends that the "connection request" described in this passage is a "management request" within the meaning of Claim 2, but the plain meaning of these terms is entirely different. Even if the connection request is a management request, the connection request is not created by "the management proxy," as recited in Claim 2. Rather, the "connection request is received from client 214 or server 216. Therefore, *Green* does not teach or suggest that the management proxy performs the step of "based at least upon the request from the management application, creating a management request."

This element is also missing from *Davies*. In fact, the Office Action did not even allege that *Davies* disclosed or suggested such an element.

(2) *Davies* does not teach "storing said management request in the management proxy while awaiting a poll for the management request from the network entity."

Claim 2 also recites "storing said management request in the management proxy while awaiting a poll for the management request from the network entity." The Office Action admits that *Green* does not teach or suggest such a feature. Rather, the Office Action alleges that

Davies teaches such a feature at col. 10, lines 61–66, because “the connection request is stored until the poller sends a Get request command.”

Davies contains no such teaching. The cited passage only states that an “input module 701 stores information concerning interface 764.” There is no evidence that this information is a “management request.” Nor is there any evidence that this information is stored “while awaiting a poll message.” While input module 701 may later receive an SNMP Get Request 755, the Get request has absolutely no relationship to the information stored concerning 764—certainly *Davies* says nothing about storing this information “until” the Get request 755 is received. In fact, the SNMP Get Request 755 is not even a poll message within the meaning of Claim 2, because it does not “request from the management proxy any available management requests applicable to the network entity.”

(3) *Davies* does not teach a “poll message requesting from the management proxy any available management requests applicable to the network entity.”

Claim 2 also recites “receiving a poll message from the network entity, said poll message requesting from the management proxy any available management requests applicable to the network entity.” The Office Action again admits that *Green* does not teach or suggest such a feature. Rather, the Office Action alleges that *Davies* teaches such a feature in *Davies* at col. 11, lines 16–30, because “the poll request gets a response by an interface that receives that message.”

Davies contains no such teaching. This passage of *Davies* states that in response to an interface receiving a poll request, the interface stores information. This passage says nothing about a management proxy receiving the poll request. Nor is there any evidence that the poll message “request[s] from the management proxy any available management requests applicable to the network entity.” In fact, given that the only action taken in response to the poll request is that the interface stores information, it is abundantly clear that the poll request does not “request from the management proxy any available management requests applicable to the network entity.”

(4) *Davies* teaches neither “selecting one or more management requests” nor “delivering the selected one or more management requests.”

Claim 2 also recites “selecting one or more management requests stored in the management proxy that match the network entity,” and then “delivering the selected one or more management requests to the network entity.” The Office Action again admits that *Green* does not teach or suggest such steps. Rather, the Office Action alleges that *Davies* teaches such steps in *Davies* at col. 3, lines 35–43, because “after a query message is polled, a response message is sent to the server stating a[n] interface is reachable.”

The allegation is in error. This passage of *Davies* does not teach or suggest anything about a “management request” stored at a “management proxy,” much less selecting a management request and delivering that management request to a network entity. ***Davies’* response message contain no management request, only data stating that an interface is reachable.**

For at least the foregoing reason, the combination of *Green* and *Davies* fails to provide the complete subject matter recited in independent Claim 2. Therefore, the combination of *Green* and *Davies* would not have rendered Claim 2 obvious under 35 U.S.C. § 103. Reconsideration is respectfully requested.

CLAIM 43

Independent Claim 43 also recites features argued above with relation to Claim 2, although Claim 43 is expressed in another format. Because Claim 43 has at least one of the features described above for Claim 2, Claim 43 is therefore allowable over the combination of *Green* and *Davies* for at least one of the same reasons as given above for Claim 2. Reconsideration is respectfully requested.

CLAIMS 3–6, 29–32, 38–41, 44–47, 49–52, AND 58–61

Each of Claims 3–6, 29–32, 38–41, 44–47, 49–52, and 58–61 is dependent upon independent Claims 1, 2, 28, 34, 42, 43, 48, or 54. As discussed in section I above, *Green* fails to teach or suggest one or more features of Claim 1, 28, 34, 42, 48 and 54. The one or more features, identified above, which are missing from *Green*, are also missing from *Davies*. In fact, the Office Action did not rely upon *Davies* for teaching the one or more features. Moreover, as

discussed above, the combination of *Green* and *Davies* fails to teach or suggest Claims 2 and 43. Consequently, the combination of *Green* and *Davies* fails to teach or suggest one or more features of Claims 3–6, 29–32, 38–41, 44–47, 49–52, and 58–61. Thus, Claims 3–6, 29–32, 38–41, 44–47, 49–52, and 58–61 are patentable over the combination of *Green* and *Davies*.

Additionally, each of the dependent claims recites at least one additional feature that independently renders it patentable over the combination of *Green* and *Davies*. However, to expedite prosecution in light of the fundamental differences already identified, further arguments for each independently patentable feature of Claims 3–6, 29–32, 38–41, 44–47, 49–52, and 58–61 are not provided at this time. Applicants reserve the right to further point out the differences between the cited art and the novel features recited in the dependent claims.

III. CONCLUSION

For the reasons set forth above, all of the pending claims are now in condition for allowance. The Examiner is respectfully requested to contact the undersigned by telephone relating to any issue that would advance examination of the present application.

A petition for extension of time, to the extent necessary to make this reply timely filed, is hereby made. If any applicable fee is missing or insufficient, throughout the pendency of this application, the Commissioner is hereby authorized to charge any applicable fees and to credit any overpayments to our Deposit Account No. 50-1302.

Respectfully submitted,
HICKMAN PALERMO TRUONG & BECKER LLP

Date: January 14, 2009

/KarlTRees#58983/
Karl T. Rees, Reg. No. 58,983

2055 Gateway Place, Suite 550
San Jose, CA 95110
(408) 414-1233
Facsimile: (408) 414-1076